DIGITAL SIGNATURE SYSTEM, DIGITAL SIGNATURE METHOD, DIGITAL SIGNATURE MEDIATION METHOD, DIGITAL SIGNATURE MEDIATION SYSTEM, INFORMATION TERMINAL AND STORAGE MEDIUM

ABSTRACT

The present invention provides digital signature techniques using an information terminal, such as a portable terminal, having limited calculation resources. In one embodiment, a signature demandant generates a document to be signed, and an agent receives this document. The agent generates summary text for this document, and transmits the summary text to a signatory, and the signatory displays the summary text using his or her information terminal. The signatory confirms the contents, employs a private key stored in his or her terminal to sign (encrypt) the summary text. The signatory thereafter transmits a signature value to the agent, who generates a signed document that includes the signature value. Finally, the signature demandant verifies (decrypts) the received signed document using the public key of the signatory and confirms the contents.